REMARKS

Claims 1, 2, 4, 6-18, and 20-35 are currently pending in the subject application and are presently under consideration. Claims 1, 15, 18, 20, 28 and 33-35 have been amended as shown on pp. 2-9 of the Reply. Claims 17 and 32 have been canceled.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Objection of Claims 15, 17, 31, 34 and 35

In the Final Office Action dated December 12, 2008, claims 15, 17, 31, 34 and 35 stand objected to because of various informalities. Claims 15, 17, 31, 34 and 35 have been amended to correct any deficiencies related to this objection, as such the objection is moot and should be withdrawn.

II. Rejection of Claims 1, 20, 28 and 33-35 Under 35 U.S.C. §112

In the Final Office Action dated December 12, 2008, claims 1, 20, 28 and 33-35 stand rejected under 35 U.S.C. §112, second paragraph as having insufficient antecedent basis for the limitation "the sequence of one of the messages". Claims 1, 20, 28 and 33-35 have been amended to correct any deficiencies related to this rejection, as such the rejection is moot and should be withdrawn.

III. Rejection of Claims 1-2, 4, 6, 14-18, 20, 28 and 30-35 Under 35 U.S.C. §103(a)

In the Final Office Action dated December 12, 2008, claims 1-2, 4, 6, 14-18, 20, 28 and 30-35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Venkatesan *et al.* (US 6,829,710). It is respectfully requested that this rejection should be withdrawn for at least the following reasons. Moskowitz and Venkatesan *et al.*, individually or in combination, do not teach or suggest each and every element as set forth in the subject claims.

The claimed subject matter relates to a first code that is designed within the noise model, and performs various algebraic transformations on such first code to create a second code. Upon transforming the first code into the second code, the second code will appear to be random to a computationally bounded adversary. Therefore an adversarial attack on the second code will

essentially be a noise attack on the first code, as the attack will be randomly distributed across the first code. Randomly distributing the attack across the first code allows the code to act as it was designed – with respect to random noise. Thus the first code can be associated with error correction/detection properties when random noise is applied to the first code.

Independent claim 1 recites a system that facilitates efficient code construction, comprising: *a component that receives a first code designed in a noise model,...; and a transformation component that transforms the first code to a new code that has essentially same length parameters as the first code but is hidden to a computationally bounded adversary, ..., wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code by the computationally bounded adversary would appear as a noise attack on the first code, this allows the first code to utilize the algorithms to correct the noise errors;...; and a tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code; and* ***a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and further generates a random permutation σ that permutes the n bits***. The cited references do not expressly or inherently disclose the aforementioned novel aspects of applicants' claimed subject matter as recited in the subject claims.

Moskowitz discloses a system for encoding digital watermark information in a signal. The system includes a window identifier for identifying a sample window in the signal; an interval calculator for determining a quantization interval of the sample window; and a sampler for normalizing the sample window to provide normalized samples. Further, the system includes a processor for identifying an area of the digital signal that will be affected by the digital filter and an encoder for encoding the at least one digital watermark in the digital signal. The encoder encodes the digital watermark so as to avoid the area of the digital signal that will be affected by the digital filter. (*See* pg. 2, paragraphs [0010]-[0011]).

In contrast, applicants' claimed subject matter discloses a system that includes a code generator that generates a code designed in a noise model. The code is then relayed to a code

hiding module that facilitates randomizing the code, thereby hiding the code from potential and/or actual adversaries.

More particularly, the code generator includes an encoding function *f* that encodes a plurality of messages into the code. Thus, the code is generated based upon a sequence of *t* messages m_1, m_2, m_3, …, m_i, m_{i+1}, …, m_t, where each message *m* is *k* bits in length. The code generator therefore generates the code *via* sequentially encoding each message (*e.g.*, $f(m_i)$). The code hiding module receives the code in a sequence of $f(m_1), f(m_2), \ldots f(m_i), \ldots f(m_t)$, and *via* utilizing a pseudo random number generator generates two pseudo random numbers of *n* bits, *a* and *b* for each encoded message, where $a \neq 0$. These pseudo random numbers are generated based upon a position within the sequence of each encoded message *m*. The code-hiding module also utilizes the pseudo random generator to generate a random permutation σ to permute *n* bits. The code-hiding module can then send $a \times \sigma(f(m_i)) + b$ (*e.g.*, code 2), where × is a bitwise multiplication operator, over a channel and to a receiver that includes a decoder. While resident within the channel, a noise vector can be added to code 2. For example, a vector *v* (adversarial in nature) of Hamming weight *w* can be added to code 2 by the channel. Therefore the decoder receives $a \times \sigma(f(m_i)) + b + v$. (*See* pg. 12, lines 13-27).

Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages, and further generates a random permutation. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. Further, Moskowitz does not disclose a first code generated based at least in part on a sequence of messages.

Venkatesan *et al.* does not cure the deficiencies of Moskowitz. Venkatesan *et al.* discloses an apparatus for forming and embedding a highly tamper-resistant cryptographic identifier, *i.e.*, a watermark, within non-marked executable code. Since the flow pattern of the watermark is highly intertwined with the flow pattern of the non-marked code, the watermark is effectively impossible to either remove from the code and/or circumvent. The routines are added in such a manner that the flow pattern of resulting watermarked code is not substantially

different from that of the non-marked code, thus frustrating third party detection of the watermark using standard flow analysis tools. (*See* col. 3, lines 6-23).

Venkatesan *et al.* does not disclose a system that generates a code *via* sequentially encoding each message, as in applicants' claimed subject matter. The pseudo random number generator then generates two pseudo random numbers of *n* bits, *a* and *b* for each encoded message. These pseudo random numbers are generated based upon a position within the sequence of each encoded message *m*. Venkatesan *et al.* merely discloses a generator that randomly selects pairs of nodes in the flow graphs and inserts an edge between the nodes in each pair. Venkatesan *et al.* does not disclose utilizing a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages, and further generates a random permutation. Venkatesan *et al.* simply provides for traversing the flow graphs by visiting all the nodes in a predetermined sequence or possible nodes may be pseudo randomly selected for omission. Accordingly, Venkatesan *et al.* does not disclose ...***a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and further generates a random permutation*** σ ***that permutes the n bits***.

Furthermore, independent claim 20 recites a system that hides a codeword from a computationally bounded adversary, comprising: ...*; a tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code; and* ***a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and further generates a random permutation*** σ ***that permutes the n bits***.

As stated *supra*, Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages, and further generates a random permutation. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. And, Venkatesan *et al.* does not disclose a system

that generates a code *via* sequentially encoding each message, as in applicants' claimed subject matter. The pseudo random number generator then generates two pseudo random numbers of *n* bits, *a* and *b* for each encoded message. These pseudo random numbers are generated based upon a position within the sequence of each encoded message *m*. Venkatesan *et al.* merely discloses a generator that randomly selects pairs of nodes in the flow graphs and inserts an edge between the nodes in each pair.

Further, independent claim 28 recites a method for hiding a data package from a computationally bounded adversary, comprising:*…; utilizing the algorithms of the first code to correct the noise errors; and determining whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code; and* ***generating two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and further generating a random permutation σ that permutes the n bits***.

As stated *supra*, Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages, and further generates a random permutation. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. And, Venkatesan *et al.* does not disclose a system that generates a code *via* sequentially encoding each message, as in applicants' claimed subject matter. The pseudo random number generator then generates two pseudo random numbers of *n* bits, *a* and *b* for each encoded message. Venkatesan *et al.* simply provides for traversing the flow graphs by visiting all the nodes in a predetermined sequence or possible nodes may be pseudo randomly selected for omission.

Further, independent claim 33 recites a system that facilitates efficient code construction, comprising: ***… means for generating two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and further means for generating a random permutation σ that permutes the n bits.***

Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of

the messages, and further generates a random permutation. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. And, Venkatesan *et al.* does not disclose a system that generates a code *via* sequentially encoding each message, as in applicants' claimed subject matter. The pseudo random number generator then generates two pseudo random numbers of *n* bits, *a* and *b* for each encoded message. Venkatesan *et al.* merely discloses a generator that randomly selects pairs of nodes in the flow graphs and inserts an edge between the nodes in each pair.

Further, independent claim 34 recites a computer readable medium having computer executable instructions stored thereon to transfer a first code into a second code, ***… a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within a sequence of one of the messages, and further generates a random permutation σ that permutes the n bits***.

Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. And, Venkatesan *et al.* does not disclose a system that generates a code *via* sequentially encoding each message, as in applicants' claimed subject matter. The pseudo random number generator then generates two pseudo random numbers of *n* bits, *a* and *b* for each encoded message. Venkatesan *et al.* simply provides for traversing the flow graphs by visiting all the nodes in a predetermined sequence or possible nodes may be pseudo randomly selected for omission.

Furthermore, independent claim 35 recites a computer readable medium having a data structure stored thereon that receives a first code that is designed in a noise model and transforms the first code into a second code, ***… a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within a sequence of one of the messages, and further generates a random permutation σ that permutes the n bits.***

Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. And, Venkatesan *et al.* does not disclose a system that generates a code *via* sequentially encoding each message, as in applicants' claimed subject matter. The pseudo random number generator then generates two pseudo random numbers of *n* bits, *a* and *b* for each encoded message. Venkatesan *et al.* merely discloses a generator that randomly selects pairs of nodes in the flow graphs and inserts an edge between the nodes in each pair.

In view of the aforementioned deficiencies of the cited references, it is respectfully submitted that this rejection be withdrawn with respect to claims 1-2, 4, 6, 14-18, 20, 28 and 30-35.

IV. Rejection of Claims 7-8, 25, and 29 Under 35 U.S.C. §103(a)

In the Final Office Action dated December 12, 2008, claims 7-8, 25, and 29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Venkatesan *et al.* (US 6,829,710), in further view of Cox (US 6,275,965). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz, Venkatesan *et al.* and Cox *et al.,* individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Cox *et al.* does not make up for aforementioned deficiencies of Moskowitz and Venkatesan *et al.* with respect to independent claims 1, 20 and 28 (which claims 7-8, 25 and 29 depend respectively there from). Thus, the claimed subject matter as recited in claims 7-8, 25 and 29 is not obvious over the combination of Moskowitz, Venkatesan *et al.* and Cox *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

V. Rejection of Claims 9 and 10 Under 35 U.S.C. §103(a)

In the Final Office Action dated December 12, 2008, claims 9 and 10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742), in view of Venkatesan *et al.* (US 6,829,710), in further view of Guruswami (Foundations of Computer

Science, 2001, Proceedings, 42nd IEEE Symposium, Pages 658-667, ISBN: 0-7695-1116-3). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz, Venkatesan *et al.* and Guruswami, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Guruswami does not make up for aforementioned deficiencies of Moskowitz and Venkatesan *et al.* with respect to independent claim 1 (which claims 9 and 10 depend there from). Thus, the claimed subject matter as recited in claims 9 and 10 is not obvious over the combination of Moskowitz, Venkatesan *et al.* and Guruswami. Therefore, it is respectfully submitted that this rejection be withdrawn.

VI. Rejection of Claims 21-23 Under 35 U.S.C. §103(a)

In the Final Office Action dated December 12, 2008, claims 21-23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742), in view of Venkatesan *et al.* (US 6,829,710), in further view of Bohnke (US 6,557,139). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz, Venkatesan *et al.* and Bohnke *et al.,* individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Bohnke *et al.* does not make up for aforementioned deficiencies of Moskowitz and Venkatesan *et al.* with respect to independent claim 20 (which claims 21-23 depend there from). Thus, the claimed subject matter as recited in claims 21-23 is not obvious over the combination of Moskowitz, Venkatesan *et al.* and Bohnke *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

VII. Rejection of Claim 24 Under 35 U.S.C. §103(a)

In the Final Office Action dated December 12, 2008, claim 24 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742), in view of Venkatesan *et al.* (US 6,829,710), in further view of Bohnke (US 6,557,139) and in further view of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages 658-667, ISBN: 0-7695-1116-3). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz, Venkatesan *et al.*, Bohnke *et al.,* and Guruswami, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Guruswami does not make up for aforementioned

deficiencies of Moskowitz, Venkatesan *et al.* and Bohnke *et al.* with respect to independent claim 20 (which claim 24 depends respectively there from). Thus, the claimed subject matter as recited in claim 24 is not obvious over the combination of Moskowitz, Venkatesan *et al.*, Bohnke *et al.* and Guruswami. Therefore, it is respectfully submitted that this rejection be withdrawn.

VIII. Rejection of Claims 26 and 27 Under 35 U.S.C. §103(a)

In the Final Office Action dated December 12, 2008, claims 26 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742), in view of Venkatesan *et al.* (US 6,829,710), in further view of Tian *et al.* (US 6,714,683). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz, Venkatesan *et al.* and Tian *et al.,* individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Tian *et al.* does not make up for aforementioned deficiencies of Moskowitz and Venkatesan *et al.* with respect to independent claim 20 (which claims 26-27 depend there from). Thus, the claimed subject matter as recited in claims 26-27 is not obvious over the combination of Moskowitz, Venkatesan *et al.* and Tian *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP588US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Marisa J. Zink/
Marisa J. Zink
Reg. No. 48,064

AMIN, TUROCY & CALVIN, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731